HEALTH IT: RIGHT TIME. RIGHT PLACE. IT'S ON.
NEW ORLEANS
HIMSS13
ANNUAL CONFERENCE & EXHIBITION

Use of Interoperability Standards and Data Segmentation to Support Patient Privacy

Johnathan Coleman, CISSP, CISM
jc@securityrs.com

Duane Decouteau
ddecouteau@edmondsci.com

The Office of the National Coordinator for
Health Information Technology

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

Learning Objectives

- During this presentation, participants will learn about the Data Segmentation for Privacy (DS4P) Standards and Interoperability Initiative. The presentation will:
  - Summarize how standards can be used to electronically enforce a prohibition on redisclosure, which helps providers and patients selectively disclose health information and ensure that the information remains confidential after it is received.
  - Provide a brief overview of an implementation approach from one of the DS4P pilots: VA/SAMHSA

Agenda

- Introduction
  - Data Segmentation: Definition and Purpose
  - Examples of Heightened Legal Privacy Protections
- Methodology
  - Standards and Interoperability Framework
  - Lifecycle
- Technical Approach
- VA/SAMHSA DS4P Pilot
- Conclusion

What is Data Segmentation?

"Process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization or individual as being undesirable to share"

Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis

Melissa M. Goldstein, JD; and Alison L. Rein, MS, Director Academy Health.
Acknowledgements: Melissa M. Heesters, JD; Penelope P. Hughes, JD; Benjamin Williams; Scott A. Weinstein, JD

Why Segment Data?

- Some healthcare information requires special handling that goes beyond the protection already provided through the HIPAA Privacy rule.

- Additional protection through the use of data segmentation emerged in part through state and federal privacy laws which address social hostility and stigma associated with certain medical conditions.*

- Data Segmentation for Privacy provides a means for electronically implementing choices made under these privacy laws.

* *The confidentiality of alcohol and drug abuse Patient records regulation and the HIPAA privacy rule: Implications for alcohol and substance abuse programs*; June 2004, Substance Abuse and Mental Health Services Administration.

Examples of Heightened Legal Privacy Protections (1)

- Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations [42 CFR Part 2] which protect specific health information from exchange without patient consent.
- State and Federal laws protecting data related to select conditions/types of data
  - Mental Health
  - Data Regarding Minors
  - Intimate Partner Violence and Sexual Violence
  - Genetic Information
  - HIV Related Information

Examples of Heightened Legal Privacy Protections (2)

- Laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs [Title 38, Section 7332, USC]
  - Sickle Cell Anemia
  - HIV Related Information
  - Substance Abuse Information

- In addition, the rule 45 CFR §164.522(a)(1)(iv), effective 3/26/2013, describes how patients may withhold any health information from health plans for services they received and paid for out-of-pocket.

Initiative Methodology: Data Segmentation for Privacy

STANDARDS & INTEROPERABILITY FRAMEWORK

The Standards & Interoperability (S&I) Framework:

- Creates a collaborative, coordinated, incremental standards process.
- Is guided by the ONC (with input from Federal Advisory Committees).
- Is enabled and led by the an open community of industry participants who are interested in solving real-world problems.

Each S&I Initiative focuses on narrowly-defined, broadly applicable challenge, tackled through a rigorous development cycle, and provides input to Federal Advisory Committees for consideration.

S&I Lifecycle

EXECUTION

S&I Initiative Phases	Typical Activities of Each Phase
Pre-Discovery	• Create Initiative Synopsis, post for public comment and incorporate feedback • Creation of Initiative Charter defining Challenge statement, key stakeholders, risks, timelines and Milestones • Definition of Goals and Outcomes
Discovery	• Creation of Use Cases and User Stories, functional requirements • Identify Interoperability gaps, barriers, obstacles and costs • Identify alternative approaches and conduct feasibility tests and prototypes • Identify existing standards, models and artifacts for harmonization
Implementation	• Create Harmonized Specifications • Create Reference Implementations • Documentation relevant to the Specifications and Reference Implementations such as training guides, design documents. • Create Operation Plan for Pilot Testing
Pilot	• Revised Harmonized Specifications • Revised Reference Implementations • Transition Plan to Open Source communities • Create Pilot technology and document policy lessons
Evaluation	• Measure Initiative Success against Goals and Outcomes • Identify best practices learned from pilots for wider scale deployment • Identify Hard and Soft Policy tools that could be considered for wider scale deployments

Data Segmentation for Privacy

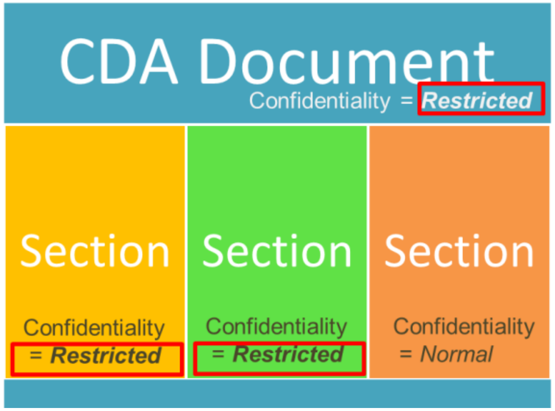
TECHNICAL APPROACH – DS4P VA/SAMHSA PILOT

Layered Approach for Privacy Metadata

- "Russian doll" concept of applying metadata with decreasing specificity as layers are added to the clinical data.
- Privacy metadata uses standards to convey:
  - Confidentiality of data in clinical payload
  - Obligations of receiving system
  - Allowed purpose of use

Types of Privacy Metadata used by DS4P

- Confidentiality Codes:
  - Used by systems to help convey or enforce rules regarding access to data requiring enhanced protection. Uses “highest watermark” approach.



CDA Document
Confidentiality = *Restricted*

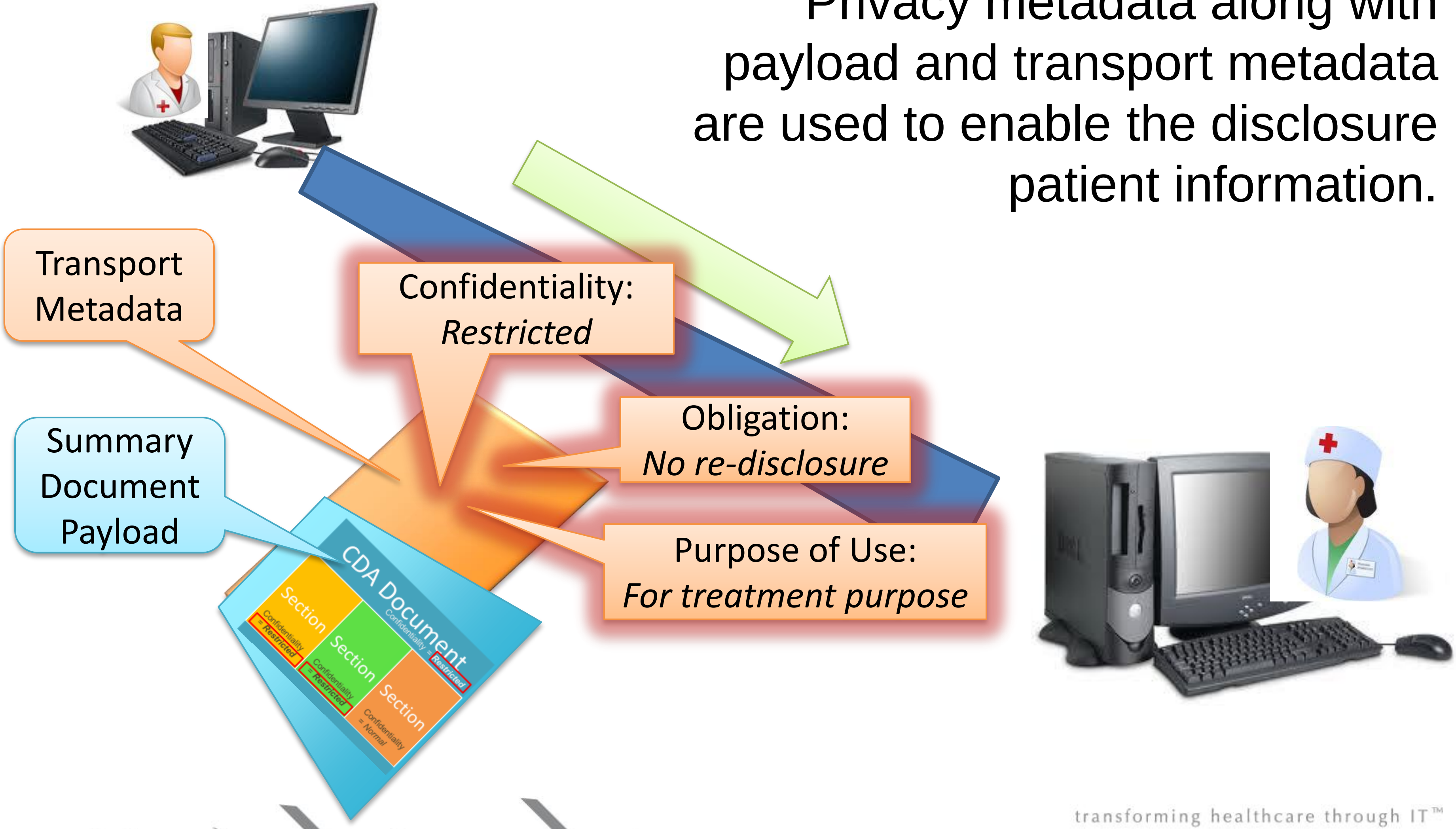
Section
Confidentiality
= *Restricted*

Section
Confidentiality
= *Restricted*

Section
Confidentiality
= *Normal*

- Purpose of Use:
  - Defines the allowed purposes for the disclosure (e.g. Treatment, Emergency Treatment etc).
- Obligations:
  - Specific obligations being placed on the receiving system (e.g. do not re-disclose without consent).

Privacy metadata along with payload and transport metadata are used to enable the disclosure patient information.



Transport Metadata

Confidentiality: *Restricted*

Obligation: *No re-disclosure*

Purpose of Use: *For treatment purpose*

Summary Document Payload

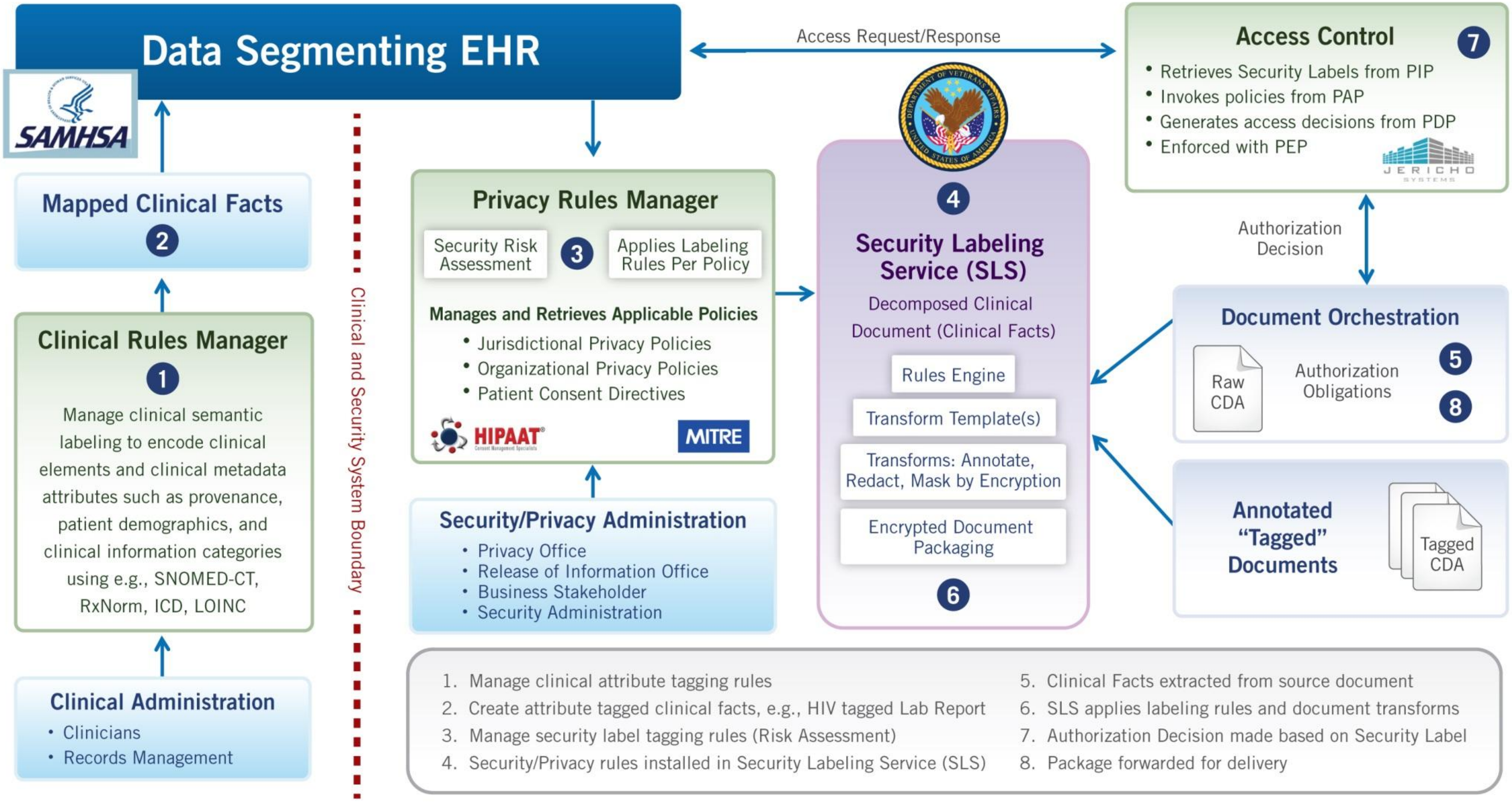
CDA Document
Confidentiality = Restricted
Section
Confidentiality = Restricted
Section
Confidentiality = Restricted
Section
Confidentiality = Normal

Data Segmentation for Privacy

VA/SAMHSA PILOT

Data Segmentation Using Healthcare Privacy and Security Labels (HIMSS 2013)

Advanced technology demonstration of the ONC Data Segmentation for Privacy Initiative, using a standards-based approach for privacy metadata to achieve interoperability and appropriate sharing of protected information, ensuring those who receive it handle it correctly.



Data Segmenting EHR

SAMHSA

Access Request/Response

Mapped Clinical Facts
2

Clinical Rules Manager
1

Manage clinical semantic labeling to encode clinical elements and clinical metadata attributes such as provenance, patient demographics, and clinical information categories using e.g., SNOMED-CT, RxNorm, ICD, LOINC

Clinical Administration
- Clinicians
- Records Management

Clinical and Security System Boundary

Privacy Rules Manager
Security Risk Assessment 3 Applies Labeling Rules Per Policy

Manages and Retrieves Applicable Policies
- Jurisdictional Privacy Policies
- Organizational Privacy Policies
- Patient Consent Directives

HIPAAT MITRE

Security/Privacy Administration
- Privacy Office
- Release of Information Office
- Business Stakeholder
- Security Administration

4

Security Labeling Service (SLS)
Decomposed Clinical Document (Clinical Facts)

Rules Engine

Transform Template(s)

Transforms: Annotate, Redact, Mask by Encryption

Encrypted Document Packaging

6

Access Control
7
- Retrieves Security Labels from PIP
- Invokes policies from PAP
- Generates access decisions from PDP
- Enforced with PEP

JERICHO SYSTEMS

Authorization Decision

Document Orchestration
Raw CDA

Authorization Obligations

5

8

Annotated "Tagged" Documents
Tagged CDA

1. Manage clinical attribute tagging rules
2. Create attribute tagged clinical facts, e.g., HIV tagged Lab Report
3. Manage security label tagging rules (Risk Assessment)
4. Security/Privacy rules installed in Security Labeling Service (SLS)
5. Clinical Facts extracted from source document
6. SLS applies labeling rules and document transforms
7. Authorization Decision made based on Security Label
8. Package forwarded for delivery

VA Consent Directive

eBenefits will be unavailable on Wednesday, 13 February from 2000-2315 EST for maintenance.

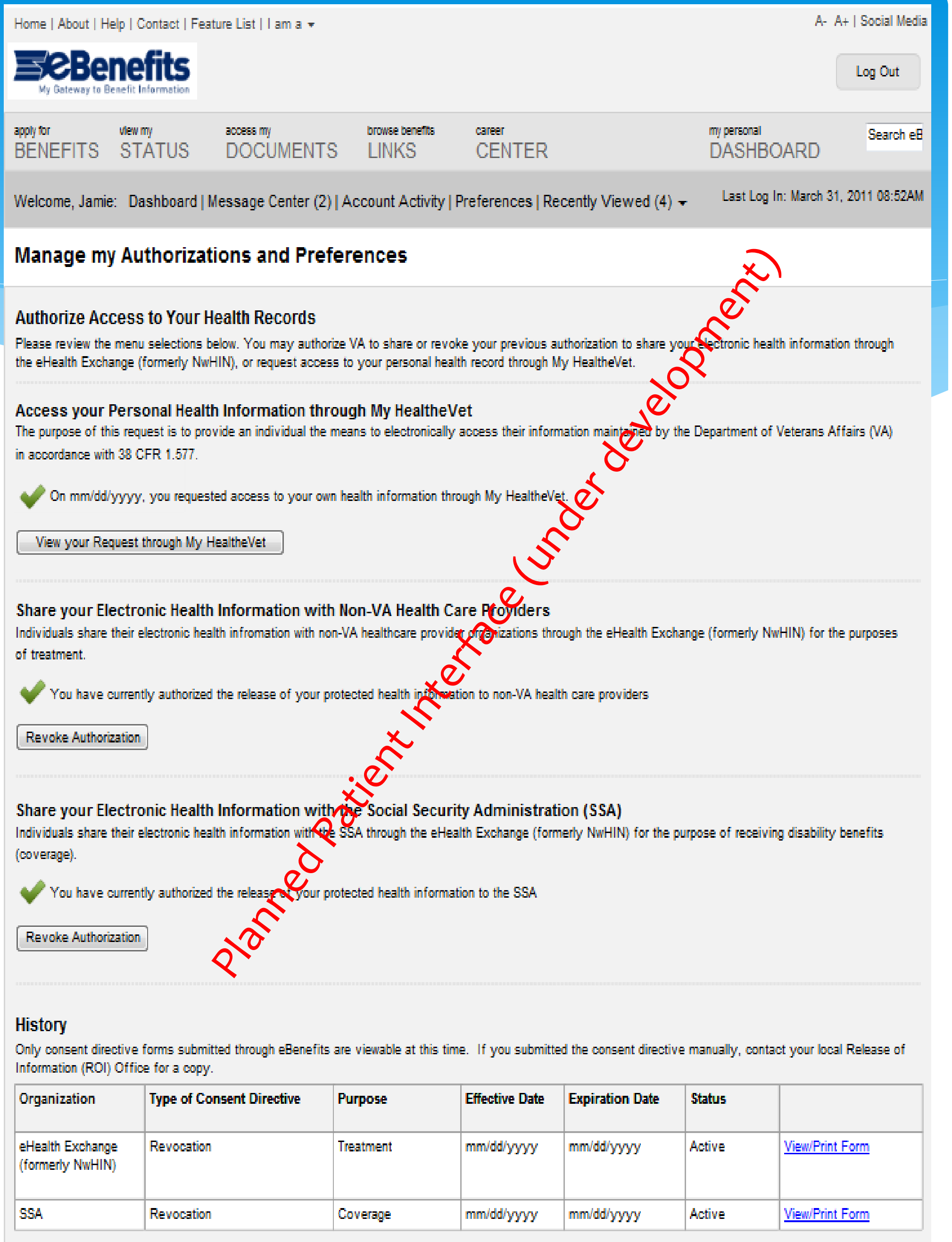
Register now to use all of the available features of eBenefits!

Your voice is important to us. Learn more about VBA's commitment to improve the benefits delivery process.

Login or register for a Premium Account to access these features.

- **VA plans to use Security Labels to enable enforcement of access restrictions authorized by the patient**
- **VA Patients will be able to create online consent directives to:**
  - **Authorize & Revoke Disclosure to eHealth Exchange and SSA**
  - **Grant Providers access to their MyHealtheVet PHR**

VA = Veterans Administration
SSA = Social Security Administration
PHR = Personal Health Record


Home | About | Help | Contact | Feature List | I am a
A- A+ | Social Media
eBenefits
My Gateway to Benefit Information
Log Out
apply for BENEFITS
view my STATUS
access my DOCUMENTS
browse benefits LINKS
career CENTER
my personal DASHBOARD
Search eB
Welcome, Jamie: Dashboard | Message Center (2) | Account Activity | Preferences | Recently Viewed (4)

Last Log In: March 31, 2011 08:52AM

Manage my Authorizations and Preferences

Authorize Access to Your Health Records

Please review the menu selections below. You may authorize VA to share or revoke your previous authorization to share your electronic health information through the eHealth Exchange (formerly NwHIN), or request access to your personal health record through My HealtheVet.

Access your Personal Health Information through My HealtheVet

The purpose of this request is to provide an individual the means to electronically access their information maintained by the Department of Veterans Affairs (VA) in accordance with 38 CFR 1.577.

✓ On mm/dd/yyyy, you requested access to your own health information through My HealtheVet.

View your Request through My HealtheVet

Share your Electronic Health Information with Non-VA Health Care Providers

Individuals share their electronic health infromation with non-VA healthcare provider organizations through the eHealth Exchange (formerly NwHIN) for the purposes of treatment.

✓ You have currently authorized the release of your protected health information to non-VA health care providers

Revoke Authorization

Share your Electronic Health Information with the Social Security Administration (SSA)

Individuals share their electronic health information with the SSA through the eHealth Exchange (formerly NwHIN) for the purpose of receiving disability benefits (coverage).

✓ You have currently authorized the release of your protected health information to the SSA

Revoke Authorization

History

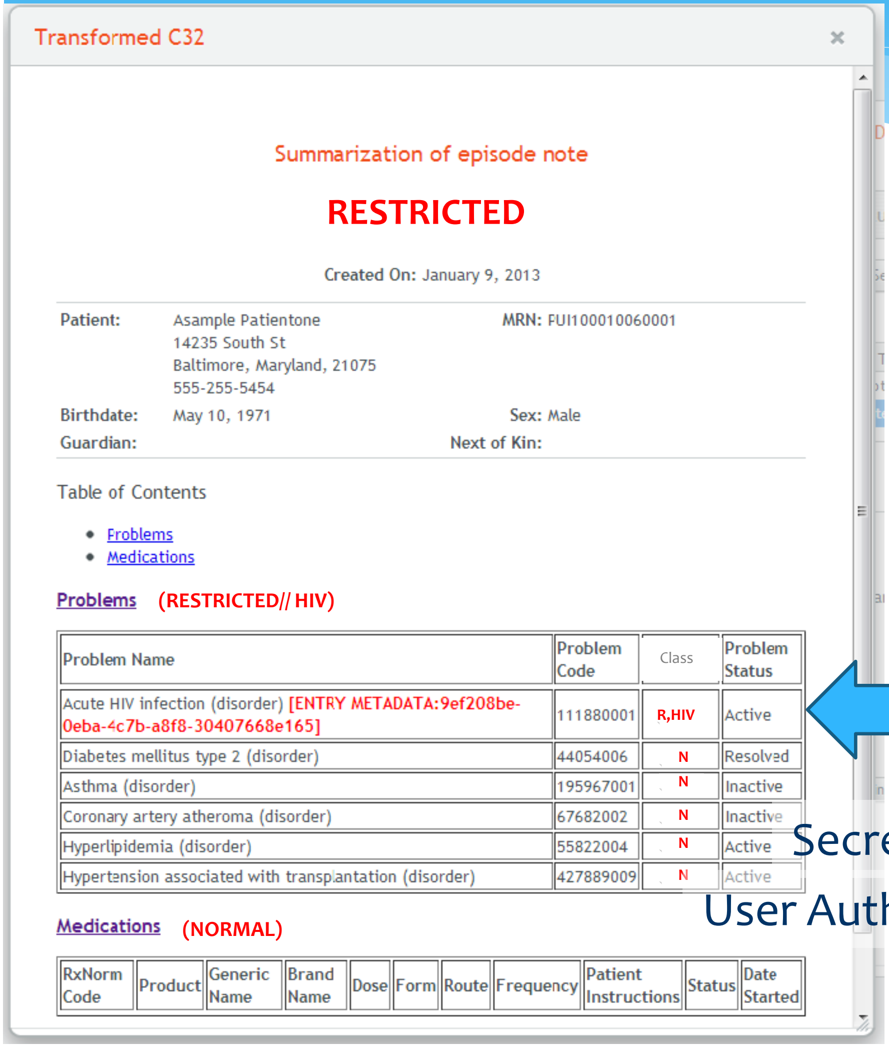
Only consent directive forms submitted through eBenefits are viewable at this time. If you submitted the consent directive manually, contact your local Release of Information (ROI) Office for a copy.

Organization	Type of Consent Directive	Purpose	Effective Date	Expiration Date	Status	
eHealth Exchange (formerly NwHIN)	Revocation	Treatment	mm/dd/yyyy	mm/dd/yyyy	Active	View/Print Form
SSA	Revocation	Coverage	mm/dd/yyyy	mm/dd/yyyy	Active	View/Print Form

Planned Patient Interface (under development)

Privacy Tagged Summary Document

UNMASKED



Transformed C32

Summarization of episode note

RESTRICTED

Created On: January 9, 2013

Patient: Asample Patientone
14235 South St
Baltimore, Maryland, 21075
555-255-5454
MRN: PUI100010060001

Birthdate: May 10, 1971 **Sex:** Male

Guardian: **Next of Kin:**

Table of Contents

- Problems
- Medications

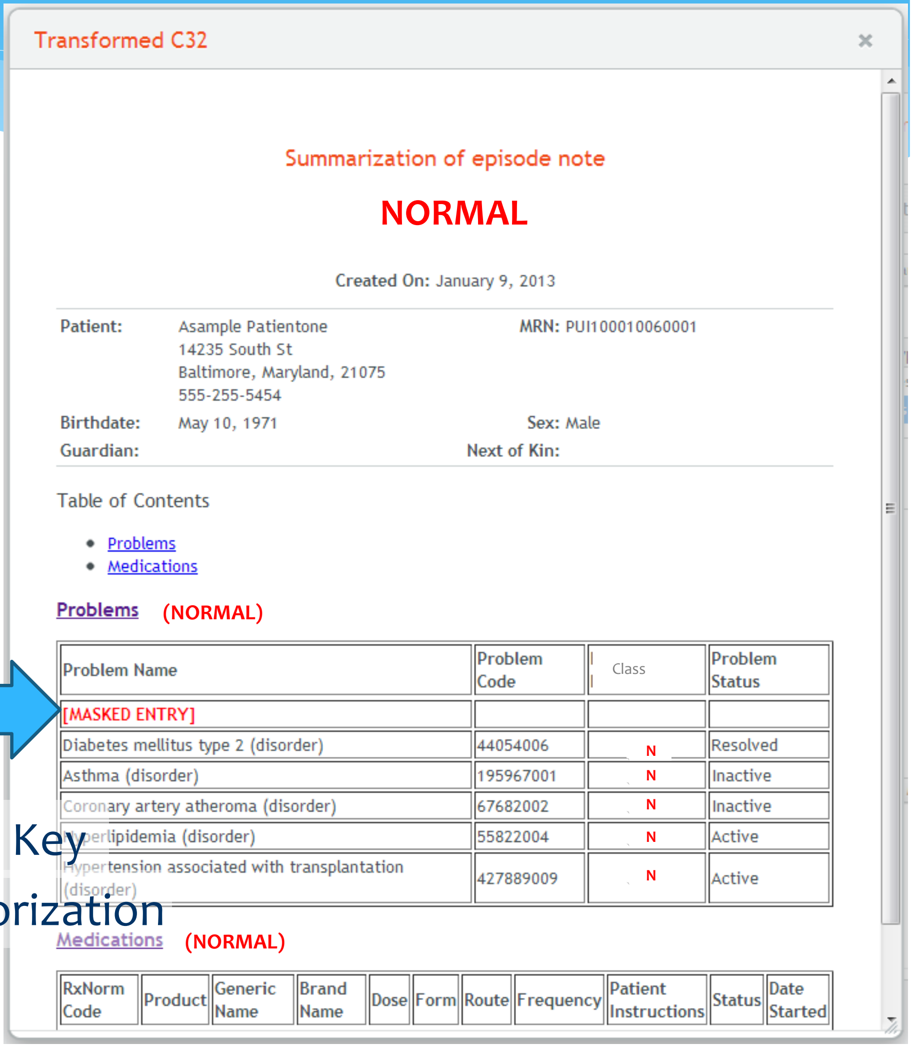
Problems **(RESTRICTED// HIV)**

Problem Name	Problem Code	Class	Problem Status
Acute HIV infection (disorder) [ENTRY METADATA:9ef208be-0eba-4c7b-a8f8-30407668e165]	111880001	R,HIV	Active
Diabetes mellitus type 2 (disorder)	44054006	N	Resolved
Asthma (disorder)	195967001	N	Inactive
Coronary artery atheroma (disorder)	67682002	N	Inactive
Hyperlipidemia (disorder)	55822004	N	Active
Hypertension associated with transplantation (disorder)	427889009	N	Active

Medications **(NORMAL)**

RxNorm Code	Product	Generic Name	Brand Name	Dose	Form	Route	Frequency	Patient Instructions	Status	Date Started

MASKED



Transformed C32

Summarization of episode note

NORMAL

Created On: January 9, 2013

Patient: Asample Patientone
14235 South St
Baltimore, Maryland, 21075
555-255-5454
MRN: PUI100010060001

Birthdate: May 10, 1971 **Sex:** Male

Guardian: **Next of Kin:**

Table of Contents

- Problems
- Medications

Problems **(NORMAL)**

Problem Name	Problem Code	Class	Problem Status
[MASKED ENTRY]			
Diabetes mellitus type 2 (disorder)	44054006	N	Resolved
Asthma (disorder)	195967001	N	Inactive
Coronary artery atheroma (disorder)	67682002	N	Inactive
Hyperlipidemia (disorder)	55822004	N	Active
Hypertension associated with transplantation (disorder)	427889009	N	Active

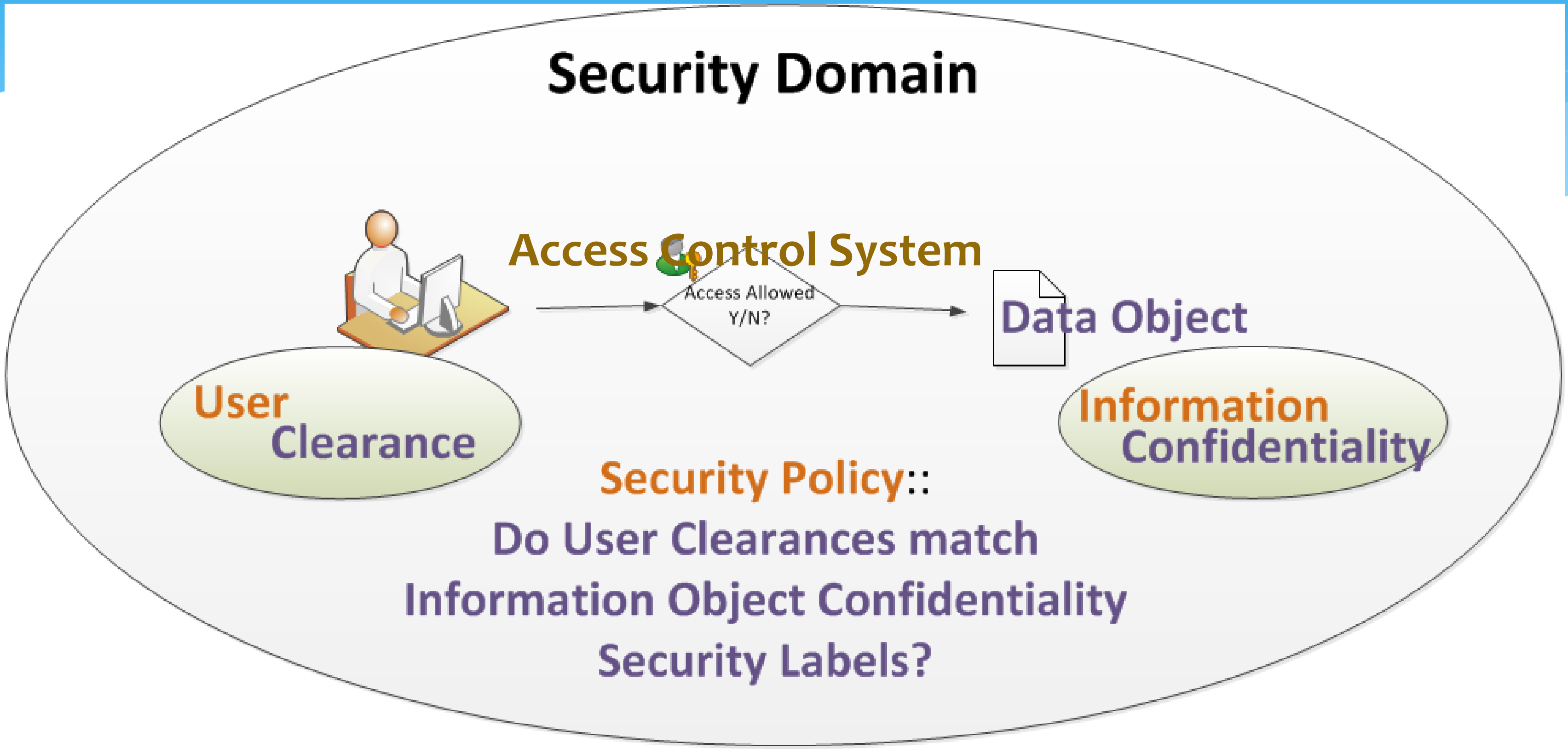
Medications **(NORMAL)**

RxNorm Code	Product	Generic Name	Brand Name	Dose	Form	Route	Frequency	Patient Instructions	Status	Date Started

Secret Key

User Authorization

Security Domain



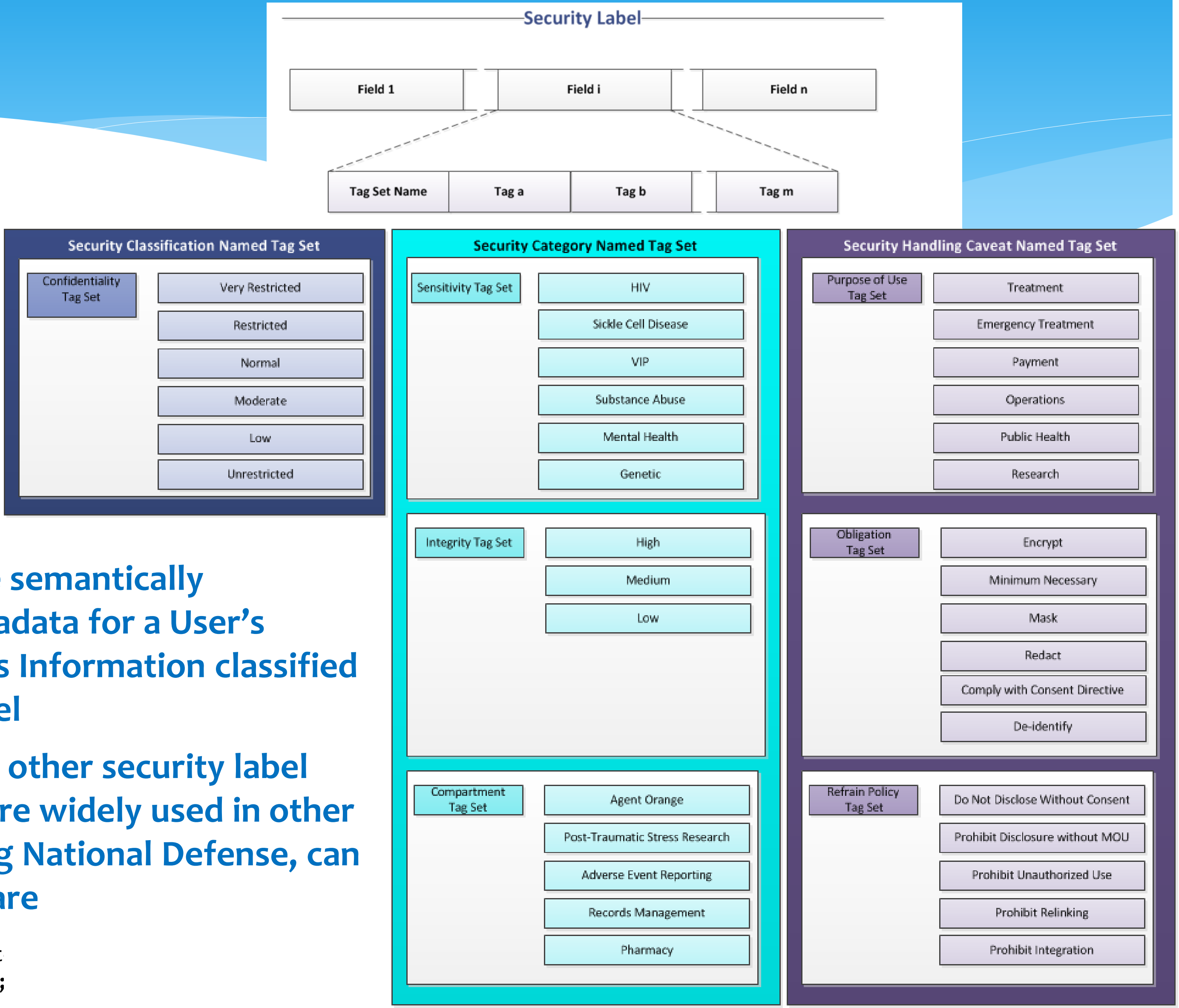
Security Label conveys Access Control Information about Users and Requested Information

- User Security Labels are called “Clearances”
- Information Security Labels are called “Classifications” such as Confidentiality and Sensitivity

NIST FIPS PUB 188 Security Labels

NEW!

Post-HIMSS



Security Label

Field 1 | Field i | Field n

Tag Set Name | Tag a | Tag b | Tag m

Security Classification Named Tag Set

- Confidentiality Tag Set: Very Restricted, Restricted, Normal, Moderate, Low, Unrestricted

Security Category Named Tag Set

- Sensitivity Tag Set: HIV, Sickle Cell Disease, VIP, Substance Abuse, Mental Health, Genetic
- Integrity Tag Set: High, Medium, Low
- Compartment Tag Set: Agent Orange, Post-Traumatic Stress Research, Adverse Event Reporting, Records Management, Pharmacy

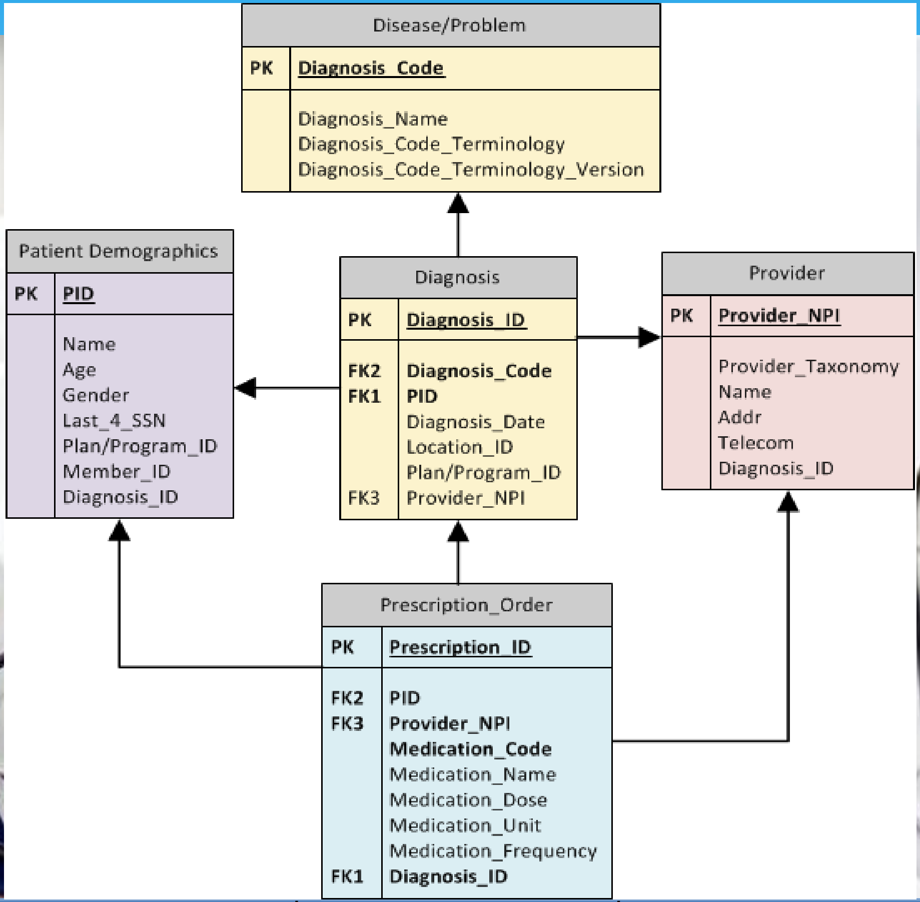
Security Handling Caveat Named Tag Set

- Purpose of Use Tag Set: Treatment, Emergency Treatment, Payment, Operations, Public Health, Research
- Obligation Tag Set: Encrypt, Minimum Necessary, Mask, Redact, Comply with Consent Directive, De-identify
- Refrain Policy Tag Set: Do Not Disclose Without Consent, Prohibit Disclosure without MOU, Prohibit Unauthorized Use, Prohibit Relinking, Prohibit Integration

- **Security Labels are semantically interoperable metadata for a User's Clearance to access Information classified with the same Label**
- **NIST, ISO, IETF and other security label standards, which are widely used in other industries including National Defense, can be used in healthcare**

NIST = National Institute of Scienc
Organization for Standardization;
Taskforce

Security Labels Bind Clinical Metadata to Patient Consent



Disease/Problem	
PK	Diagnosis_Code
	Diagnosis_Name Diagnosis_Code_Terminology Diagnosis_Code_Terminology_Version

Patient Demographics	
PK	PID
	Name Age Gender Last_4_SSN Plan/Program_ID Member_ID Diagnosis_ID

Diagnosis	
PK	Diagnosis_ID
FK2	Diagnosis_Code
FK1	PID
	Diagnosis_Date
	Location_ID
	Plan/Program_ID
FK3	Provider_NPI

Provider	
PK	Provider_NPI
	Provider_Taxonomy Name Addr Telecom Diagnosis_ID

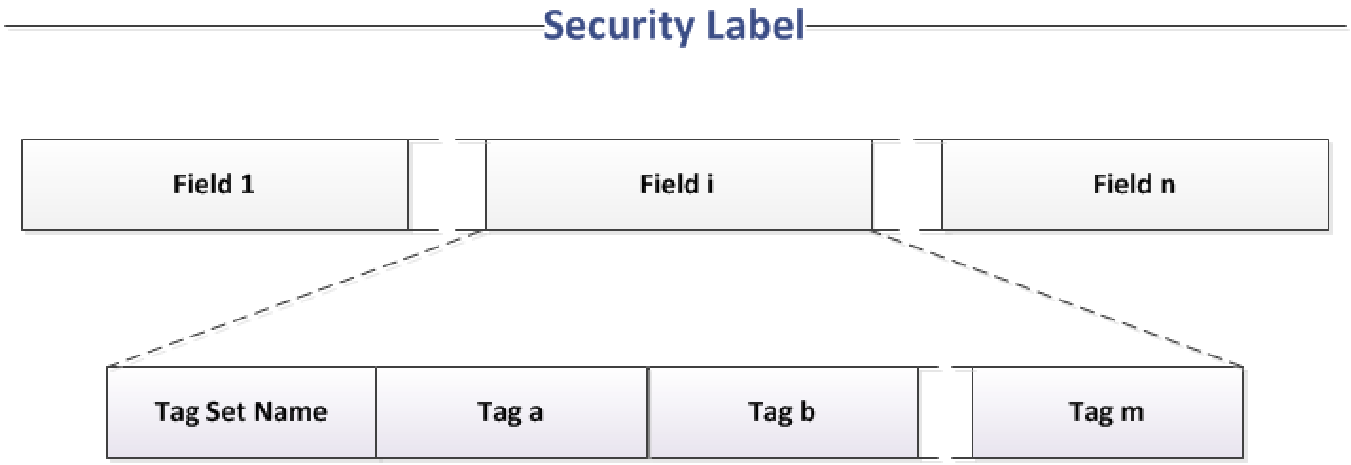
Prescription_Order	
PK	Prescription_ID
FK2	PID
FK3	Provider_NPI
	Medication_Code
	Medication_Name
	Medication_Dose
	Medication_Unit
	Medication_Frequency
FK1	Diagnosis_ID

Medication ID	Medication Name	Terminology	Confidentiality	Sensitivity
11413	AZT (Zidovudine)	RxNorm	Restricted	HIV
Diagnosis ID	Diagnosis Name	Terminology	Confidentiality	Sensitivity
111880001	Acute HIV Disorder	SNOMED	Restricted	HIV
Privacy Rule: If Diagnosis=111880001 (HIV) and Medication=11413 (Zidovudine), then Security Label Tags are Confidentiality = R and Sensitivity = HIV				

HCS Clinical Fact Metadata Example

Clinical Fact	Clinical Attribute	Provenance	Security Label
			(HL7*)
Diagnosis	<Patient Name >		N
	Source=<Organization>		N
	111880001 Acute HIV infection (disorder)	hadPrimarySource: SNOMED Code	Restricted, HIV
		wasAttributedTo: <Attending>	
Medications	<Patient Name >		N
	11413 Zidovudine (AZT)	hadPrimarySource: RxNorm	
		wasDerivedFrom: Diagnosis	Restricted, HIV
Allergies	<Patient Name >	wasDerivedFrom: Encounter	N
	91936005 (Penicillin)	hadPrimarySource: SNOMED CT	N
Laboratory Report	8053 (Lipid Panel)	hadPrimarySource: LOINC	N
	8320 Total Cholesterol		
	8316 Triglyceride		
	8429 HDL		
	7973 LDL		
Procedure	86689.Z7 (HIV-1 Western Blot)	hadPrimarySource: CPT	Restricted, HIV

NIST FIPS PUB 188 Security Labels



Field Name	Tag Set Name	Tags
Confidentiality	HL7 Confidentiality	VR (Very Restricted) R (Restricted), N (Normal), …
Sensitivity	HL7 Sensitivity Privacy Policy Type	HIV, ETH, PSY, SDV, SICKLE, …
Integrity	Integrity	High, Medium, Low
Compartment	Compartment	Agent Orange, Pharmacy, Care Team,…

- **Security Labels are semantically interoperable metadata for a User's Clearance to access Information classified with the same Label**
- **NIST, ISO, IETF and other security label standards, which are widely used in other industries including National Defense, can be used in healthcare**

NIST = National Institute of Science and Technology; ISO = International Organization for Standardization; **IETF = Internet Engineering Taskforce**

Data Segmentation for Privacy

CONCLUSION

Conclusion

- Data segmentation provides a means for protecting specific elements of health information, both within an EHR and in broader electronic exchange environments, which can prove useful in implementing current legal requirements and honoring patient choice.

Please visit the Interoperability Showcase to see live DS4P Pilot demonstrations:

VA/SAMHSA	**NETSMART**
Showcase Kiosk # 11-1	Showcase Kiosk #26-1

Federal Points of Contact

VA : **Mike Davis**, Mike.Davis@va.gov
US Department of Veterans Affairs

SAMHSA: **Richard Thoreson**, Richard.Thoreson@samhsa.hhs.gov
Substance Abuse and Mental Health Services Administration

ONC: **Scott Weinstein, J.D.** scott.weinstein@hhs.gov
Office of the Chief Privacy Officer
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services

Thank You!

Johnathan Coleman, CISSP, CISM
Initiative Coordinator, Data Segmentation for Privacy
Principal, Security Risk Solutions Inc.
698 Fishermans Bend,
Mount Pleasant, SC 29464
Tel: (843) 647-1556
Email: jc@securityrs.com

SecurityRiskSolutions
.....managing information security risks in the real world

Duane DeCouteau
Senior Software Engineer
Edmond Scientific Company
4000 Legato Road, Suite 1100
Fairfax, Virginia 22033
Tel: (703) 896-7681
Email: ddecouteau@edmondsci.com

EDMONDSCIENTIFIC COMPANY
Advanced Data Exchange Protection and Privacy